UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
A gray Honda Civic, North Carolina license plate number JDB-6899

Case No. 1:22MJ102-1

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment B

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment D

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2)	Receipt or distribution of child pornography
18 U.S.C. §§ 2252(a)(4)	Access with intent to view child pornography

The application is based on these facts:

See Affidavit of Special Agent Gabriela Dye Rees.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Gabriela Dye Rees
Applicant's signature

Gabriela Dye Rees, Special Agent (FBI)
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 03/08/2022 3:36pm

Judge's signature

City and state: Durham, North Carolina

Hon. Joe L. Webster, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Gabriela Dye Rees, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I am investigating offenses related to child sexual exploitation. This Affidavit is submitted in support of an application for a warrant to search the premises located at 21720 Bunch Road, Laurel Hill, North Carolina 28351, to include sheds and outbuildings ("SUBJECT PREMISES"), more specifically described in Attachment A, a gray Honda Civic, North Carolina license plate number JDB-6899, ("SUBJECT VEHICLE"), more specifically described in Attachment B, and QUENTIN LORAN MCLEAN, date of birth December 4, 1977 ("SUBJECT PERSON"), more specifically described in Attachment C, for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(5)(B) and 2252A(a)(2)(A), which items are more specifically described in Attachment D.

2. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every

fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located at the SUBJECT PREMISES, SUBJECT VEHICLE and SUBJECT PERSON.

AFFIANT BACKGROUND

3. I have been employed as a Special Agent of the FBI since October of 2019 and am a graduate of the eighteen-week FBI Basic Field Training Course for special agents in Quantico, Virginia. I am currently assigned to the Fayetteville Resident Agency of the Charlotte, North Carolina Division where I am responsible for investigations involving the production, advertisement, receipt, distribution and possession of child pornography, and online enticement of minors. I have received training in the area of child pornography and child sexual exploitation as well as specialized instruction on how to conduct investigations of child sexual exploitation and child pornography crimes. I have observed and reviewed numerous examples of child pornography, as defined in 18 U.S.C. § 2256. I am also familiar with, and have employed, investigative techniques used in these investigations, such as analysis of Internet Protocol addresses and Internet Service Provider records. Moreover, I

am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2252A, and I am authorized by law to request a search warrant. As a Special Agent, I am authorized to investigate violations of laws and to execute warrants issued under the authority of the United States.

STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

   a. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute.

   b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means,

including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment D:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made

or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks,

external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

i. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide

individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

j. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

k. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

l. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. "Remote computing service", as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

n. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether

between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

o. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

p. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

q. A "Virtual Private Network" or "VPN," as used herein, refers to the opportunity to establish a protected network connection when using public networks.

r. "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

BACKGROUND ON KIK MESSENGER

6. Kik Messenger (hereinafter "Kik") is a mobile application designed for chatting or messaging owned and operated by MediaLab.AI, Inc., a United States based holding company of Internet brands. Kik was formerly owned by Kik Interactive, Inc., a Canadian based company. MediaLab.AI, Inc., acquired the Kik application in October 2019.

7. According to "Kik's Law Enforcement Guide," revised in January 2021, to use the Kik application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user is asked to supply an email address; however, the email address does not have to be verified in order to use the application. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. While messaging, users can then send each other text messages, images, and videos.

8. According to "Kik's Law Enforcement Guide," Kik users are also able to create chat groups with a limited number of individuals to communicate in a group setting and exchange text messages, images and videos. These groups are administered by the group creator who has the authority to

remove and ban other users from the created group. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.

9. According to "Kik's Law Enforcement Guide," the information that Kik may be able to provide to law enforcement pursuant to a search warrant includes the following:

   a. Basic Subscriber Data: Current first and last name and email address, Link to the most current profile picture or background photo, Device related information, Account creation date and Kik version, Birthdate and email address used to register the account.

   b. Transactional Chat Log: Log of all the messages that a user has sent and received, including sender username, receiver username(s), timestamps, IP of the sender and word count (does not include the actual message that was sent).

   c. Chat Platform Log: Log of all the media files that a user has sent and received, including sender username, receiver username(s), timestamps, IP of the sender, media type, and content ID.

   d. Photographs and/or Videos: Media files sent or received by the user for last 30 days.

e. Abuse Reports: Transcript of reported chat history against the subject user, including sender username, receiver username, timestamps, actual message, and content IDs.

f. Email Events: Log of all the emails that have been associated with a username.

g. Registration IP: IP address associated to the username when the account was registered, including timestamp.

PROBABLE CAUSE

Background of investigation

8. On October 28, 2021, a FBI Online Covert Employee ("OCE"), who is a member of the FBI Child Exploitation and Human Trafficking Task Force in Jacksonville, Florida, was connected to the Internet on several occasions in an online undercover capacity from a mobile device. While using Kik, a free mobile application that permits users to send messages and other content including videos and images to other users, the OCE engaged in a private message conversation with Kik username johnman772.

9. On October 28, 2021, johnman772 posted a notice in a Kik public chat room titled "#dauluvsstrangecok" that read "Aye I'm active with my all daughters 4,7,8 I have REAL pics and vids of them if you wanna trade pm me".

10. The OCE contacted johnman772 using the private message feature of the application and a conversation ensued. During this private message conversation, the OCE took on the persona of an adult male with an 11-year-old daughter.

11. During the private message conversation on October 28, 2021, johnman772 told the OCE he was a 44-year-old male who had "vids to trade" and subsequently distributed three videos of child pornography to the OCE. The conversation between the OCE and johnman772 was as follows:

a. OCE: Hey

b. **johnman772**: Hey

c. OCE: Asl

d. **johnman772**: M44

e. OCE: U have a dau?

f. **johnman772**: [An 18 second video with sound, of a prepubescent minor female, based on the child's complete absence of pubic hair and child-sized hands, laying on her back. The child is not wearing any pants or underwear and her legs are spread, fully exposing her vagina, making it the focal point of the video. An adult male continually inserts his penis into the child's vagina throughout the duration of the video].

g. OCE: That urs?

h. **johnman772**: Yea
You?

i. OCE: Yea right u lie

j. **johnman772**: Ok
I got plenty of stuff in general I'd you wanna trade

k. OCE: Yea I've seen that vid before

l. **johnman772**: You don't wanna trade
I got some stuff
Not interested?

m. OCE: Yea looking for a real dau tho

n. **johnman772**: Can I see some
I got more stuff
?

o. OCE: U already lied about having a dau so it's hard to trust u bro

p. **johnman772**: [A 14 second video of a prepubescent minor female, based on the child's facial features and child-sized hands, sitting on what appears to be a bed. An adult male is continually inserting his penis into the child's mouth, making it the focal point of the video].
?
Guess not

q. OCE: Bro u still lied so I don't know what to tell u

r. **johnman772**: I got vids to trade

s. OCE: How much

t. **johnman772**: Like 10

u. OCE: Like those other two or different

v. **johnman772**: Yea
[A one minute 48 second video of a minor female, sitting on a bed in front of a fully nude adult male. The child is continually inserting the adult male's penis into her mouth throughout the

duration of the video. About 20 seconds into the video, the adult male removes the child's shirt and she is fully nude for the rest of the video].

12. As demonstrated in the provided descriptions above, there is probable cause to believe that johnman772 distributed at least three videos that meet the federal definition of child pornography.

Identification of Kik username "johnman772"

13. On October 29, 2021, an administrative subpoena was served to MediaLab.AI Inc. requesting subscriber information and recent IP addresses associated with Kik username Johnman772. MediaLab.AI Inc. provided the following subscriber information:

a. Display name: "John Man"
Unconfirmed email address: "johnman772@yahoo.com"
Historical IP logs, including IP addresses and date/ time of account logins

14. IP logs provided by MediaLab.AI Inc. all appear to resolve to a Kik user in the United States. On November 3, 2021, an administrative subpoena was served to Charter Communications requesting subscriber information for IP address 71.68.249.140 October 28, 2021 at 21:21 PM UTC, the same date and time johnman772 was active on Kik. Charter Communications provided the following subscriber information for the IP address:

a. Subscriber Name: Quentin Mclean
Service Address: 21720 Bunch Rd, Laurel Hill, NC 28351-8758

User Name or Features: tamelamcean40@aol.com
Phone number: 910-706-7013
Lease Log: Start Date: 02/19/2021 05:02 PM, End Date: 11/04/2021 06:40 PM

15. Based on my knowledge and experience, the Charter Communications IP address for a given account will not change between the start and end dates listed as the "Lease Log" dates. Furthermore, Charter Communications customers are serviced utilizing a "static IP address" system, which means that the IP address does not change from moment to moment or hour to hour, as it would in the case of a "dynamic IP address" system. Due to Charter Communications utilizing static IP technology, the IP address would not have changed for the target subscriber between the start and end of the "Lease Log" assignments. Therefore, QUENTIN LORAN MCLEAN would have been the subscriber associated with IP address 71.68.249.140 during the entire period from February 19, 2021 at 5:02 PM to at least November 4, 2021 at 6:40 PM, which includes October 28, 2021, the day the IP address was used by Kik username johnman772 to distribute child pornography to the FBI OCE.

16. On November 3, 2021, an administrative subpoena was served to Verizon requesting subscriber information for Natting IP addresses 174.253.129.10 on 10/28/2021 at 21:00:41 UTC (port 16820), 174.253.130.88 on 10/28/2021 at 23:53:13 UTC (port 16995), and

174.250.176.77 on 10/29/2021 at 04:46:19 UTC (port 9424), all of which were provided by MediaLab.AI Inc.

17. Information provided by Verizon stated Natting Router IP addresses can have many users at the same time, however, each Natting IP is associated with a unique phone number. Verizon confirmed the Natting IP addresses requested by the FBI are associated with phone number 910-706-7013, the same phone number listed on subscriber information received from Charter Communications. No subscriber information was available for the Natting IP addresses associated with phone number 910-706-7013 because the associated phone number is leased to Tracfone- a prepaid, no-contract mobile phone provider. Verizon does not retain subscriber data for phone numbers leased to Tracfone.

18. Database searches and North Carolina DMV records identified individuals who reside at 21720 Bunch Rd, Laurel Hill, NC 28351-8758. One of the residents, QUENTIN LORAN MCLEAN, date of birth December 4, 1977, is a 44-year-old male, the same age johnman772 self-identified as. Based on my knowledge and experience in working child pornography cases, individuals involved in the production, possession and/ or distribution of child pornography often attempt to mask their identities by creating usernames that do not relate to their true names.

However, these individuals sometimes still provide true facts or identifying information about themselves, such as their age and/ or gender, to others. These individuals likely believe that their identity will not be revealed even though they provide these basic facts to others.

19. The below vehicles were present at the SUBJECT PREMISES during spot checks from approximately January 28, 2022 to present:

a. Silver Chevrolet Malibu, North Carolina license plate number JEZ-1842. North Carolina DMV information revealed the registered owner of this vehicle is TAMELA EVETTE MCLEAN, date of birth 06/20/1979, address 21720 Bunch Road, Laurel Hill, North Carolina.

b. Dark blue Dodge Avenger, North Carolina license plate number TDS-8378. North Carolina DMV information revealed the registered owner of this vehicle is HATTIE TYSON MCLEAN, date of birth 06/22/1948, address 405 Honey Street, Laurinburg, North Carolina.

c. Gray Honda Civic, North Carolina license plate number JDB-6899. North Carolina DMV information revealed the registered owner of this vehicle is QUENTIN LORAN MCLEAN, date of birth 12/04/1977, address 21720 Bunch Road, Laurel Hill, North Carolina.

20. As further described in paragarph 22, below, individuals who have a sexual interest in children or images of children often maintain their collections in a safe, secure and private environment, such as a computer or cellphone, and are often maintained for several years and are kept close by, usually at the collector's residence, on the collector's person, in the collector's vehicle, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection.

21. Based on Kik username johnman772 self-identifying as a 44 year old male, subscriber IP information resolving to the SUBJECT RESIDENCE where a 44 year old male resides, who is the same age and gender as the SUBJECT PERSON, and the identification of shared child pornography known to me, there is probable cause to believe there is evidence of possession of child porongraphy, in violation of Title 18 U.S.C. § 2252A(a)(5)(B), and distribution of child pornography, in violation of 18 U.S.C. § 2252A(a)(2)(A), through computers and/ or devices, are located at the SUBJECT PREMISES, in the SUBJECT VEHICLE and on the SUBJECT PERSON.

CHILD PORNOGRAPHY OFFENSES IN MODERN TECHNOLOGY

22. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that

individuals who utilize the internet to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location, such as on their person or in their vehicles. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer or cellphone, and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, on the collector's person, in the collector's vehicle, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share

information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers, cell phones and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer-to-Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, Internet Relay Chat (IRC), or chat rooms or messaging services, such as Kik, have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged period of time. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

23. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these

wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers, smartphones and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children. Additionally, child pornography is not "used up" as other types of contraband can be such as alcohol or drugs. Collections can be maintained on or off-site for years at a time without the "staleness" issues of other crime types. Computers, smartphones, and the internet serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

c. Smartphones have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smartphone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smartphone can also easily plug the device into a computer (via a USB cable) or connect with a computer via Bluetooth, and transfer data files from one digital device to another. Some "smartphone" users can and do create, communicate, upload, and download child pornography, and

communicate with children to coerce them or entice them to produce child pornography or perform sexual acts, by using internet based social media or electronic service providers like Instagram, Snapchat, or Apple (and many others).

d. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo, and Google, LLC, Facebook, Dropbox, Instagram, Kik, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of

computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is maintained on the servers of the providers and is occasionally retained by the providers after the user deletes the data from their account.

f. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

g. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be

recoverable months or years later using readily available forensic tools.

h. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over terabytes of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

i. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and on the evidence of known Internet-based communications further described below, there exists a fair probability that evidence regarding the production, distribution, receipt and possession of child pornography will be found within digital devices located on the SUBJECT PREMISES, in the SUBJECT VEHICLE and/ or on the SUBJECT PERSON, or on yet-unknown digital accounts which will only be discovered through service of this search warrant and further investigation.

SEARCHING COMPUTER SYSTEMS

24. As described here and in Attachment D, this application seeks permission to search for electronic devices contained within the

SUBJECT PREMISES, SUBJECT VEHICLE and SUBJETC PERSON for various forms of data contained therein. One form in which data may be stored is a computer's hard drive or functional-equivalent storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

25. I submit that if data is found in the electronic devices to be seized under this search warrant, there is probable cause to believe evidence of the crimes set forth in this affidavit will be located, for the reasons set forth above as well as at the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or

no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

26. As further described in Attachment D, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic,

electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be stored within electronic devices located within the SUBJECT PREMISES, SUBJECT VEHICLE and on the SUBJECT PERSON because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with

the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or

consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a

storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

27. Based on my training and experience, I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

28. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage,

floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for several reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, website, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer

data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises or a vehicle; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer

user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

29. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network

activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

30. Additionally, based on past investigations involving digital devices (such as cellphones), I am aware that there are significant collections of data that are potentially relevant, irrelevant, exculpatory, and/or incriminating on any digital device. Even in the case of a relatively new cellphone, initial account setup, installed telephone number, applications, storage programs, photos, videos, and other data on the device could prove to be vital to the involved investigation. Linked cloud accounts or other online identifiers could also prove vital to identifying additional off-device premises for service of new legal process for those premises' digital contents based on the newly-identified account being associated with the digital data found inside the original searched devices. In an age of increased interconnectivity and cloud-based computing technologies, it is possible that this service of process for the physical devices searchable under this warrant will only serve to identify and confirm additional electronic service providers where ultimately, the

data resides off-site and will require another search warrant for proper access.

31. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

32. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(I)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States ... that - has jurisdiction over the offense being investigated." Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,

/S/ Gabriela Dye Rees
Gabriela Dye Rees
Special Agent
Federal Bureau of Investigation

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of the written affidavit. This the 8th day of March, 2022 at 3:36pm.

THE HON. JOE L. WEBSTER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

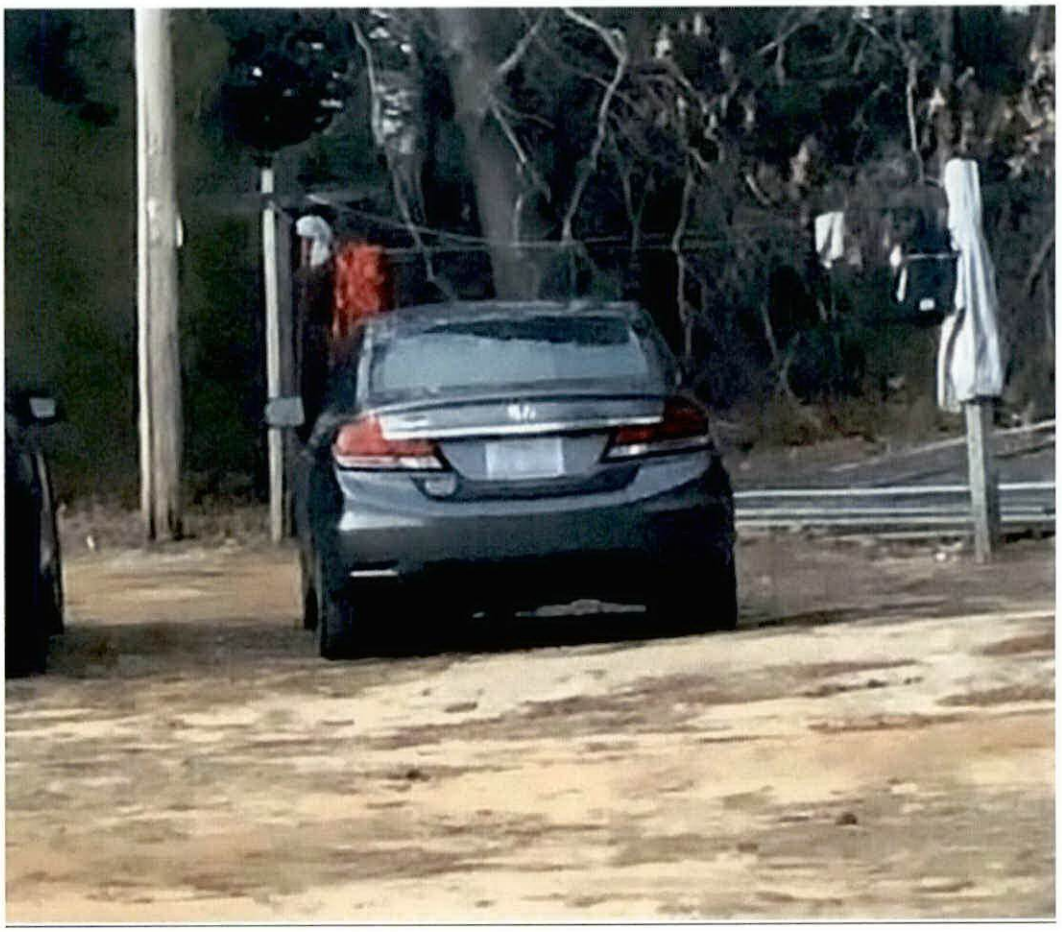
DESCRIPTION OF THE PREMISES TO BE SEARCHED

The entire premises, including sheds and outbuildings, located at 21720 Bunch Road, Laurel Hill, North Carolina 28351 ("SUBJECT PREMISES"), in the county of Scotland, in the Middle District of North Carolina. The residence on the premises is a white in color.

ATTACHMENT B

DESCRIPTION OF LOCATION TO BE SEARCHED

A gray Honda Civic, North Carolina license plate number JDB-6899 ("SUBJECT VEHICLE"), registered to QUENTIN LORAN MCLEAN, date of birth December 4, 1977.



ATTACHMENT C

QUENTIN LORAN MCLEAN ("SUBJETC PERSON")

Quentin Loran McLean, depicted above

Date of birth 12/04/1977

ATTACHMENT D

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A(a)(5)(B) and 2252A(a)(2)(A):

1. Computers or storage media that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored.
2. Routers, modems, and network equipment used to connect computers to the Internet.
3. Child pornography, as defined in 18 U.S.C. 2256(8).
4. Child erotica.
5. Records, information, and items relating to violations of the statutes described above in the form of:
    a. Records and information referencing child pornography, as defined in 18 U.S.C. 2256(8);
    b. Records and information referencing child erotica;
    c. Records, information, and items referencing or revealing the occupancy or ownership of 21720 Bunch Road, Laurel Hill, North Carolina 28351, including utility and telephone bills, mail envelopes, or addressed correspondence;
    d. Records, information and items referencing or revealing the occupancy or ownership of the gray Honda Civic, North Carolina license plate number JDB-6899, including vehicle registration card(s), vehicle title, or receipts;

e. Records and information referencing or revealing the use of peer-to-peer software, including BitTorrent client software;

f. Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;

g. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence;

h. Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved and location of occurrence;

i. Records and information referencing or revealing participation in groups or the use of services that are known to be used to facilitate the trafficking of child pornography;

j. Records and information referencing or revealing the use of remote computing services such as email, cloud storage, or online social media services.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, deleted, viewed, or otherwise interacted with;

b. evidence of how and when the COMPUTER was used to create, edit, delete, view, or otherwise interact with or engage in the things described in this warrant;

c. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

d. evidence of the Internet Protocol addresses used by the COMPUTER;

e. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

f. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

g. evidence of the lack of such malicious software;

h. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

7. During the course of the search, photographs of the location to be searched may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.